対応と回復
NetApp Ransomware Resilience

NetApp
April 14, 2026

目次

対応と回復

NetApp Ransomware Resilienceのアラートを管理する

NetApp Ransomware Resilienceは、攻撃の可能性を検出すると、ダッシュボードと通知メニューに警告を表示します。Ransomware Resilienceは直ちにスナップショットを作成します。アラートを受信した場合は、Ransomware Resilienceの*アラート*タブで潜在的なリスクを確認し、データへの影響を評価して、潜在的なランサムウェア攻撃を防止します。

Ransomware Resilienceが攻撃の可能性を検知すると、NetApp Consoleの通知設定に通知が表示され、設定されたアドレスにメールが送信されます。メールには、深刻度、影響を受けるワークロード、Ransomware Resilienceの*アラート*タブにあるアラートへのリンクが含まれます。

誤検知を無視するか、すぐにデータを回復することを決定できます。

アラートを無視すると、Ransomware Resilience はこの動作を学習し、通常の操作と関連付けて、再度アラートを開始しなくなります。

データの復旧を開始するには、アラートを復旧準備完了としてマークし、ストレージ管理者が復旧プロセスを開始できるようにします。

各アラートには、さまざまなボリュームとステータスの複数のインシデントが含まれる場合があります。すべてのインシデントを確認します。

アラートの生成方法

Ransomware Resilience は、データエントロピーパターン、ファイル拡張子の種類、暗号化に関する証拠に基づいてアラートを生成します。アラートは次のイベントに基づいています：

- データ侵害
- データ破壊
- ファイル拡張子が作成または変更されました
- 検出されたレートと予想されるレートを比較したファイルの作成
- 検出された率と予想される率の比較によるファイル削除
- 疑わしいユーザー行動
- 暗号化レベルが高く、ファイル拡張子を変更しない場合

データ侵害、データ破壊、疑わしいユーザー行動のアラートについては、"ユーザーアクティビティ検出"を設定する必要があります。

アラートの種類とステータス

アラートには、*新規*または*非アクティブ*の 2 つのステータスのいずれかがあります。

アラートは次のいずれかのタイプに分類されます：

- 潜在的な攻撃：次の場合、アラートは潜在的な攻撃として分類されます：
  - Autonomous Ransomware Protectionが新しい拡張子を検出し、過去24時間に20回以上発生した場合（デフォルトの動作）。
  - データ侵害が検出されました。
  - データ破壊が検出されました。
- 警告: 次の動作に基づいて警告が発生します。
  - 新しい拡張機能の検出はこれまで確認されておらず、同じ動作が攻撃として宣言されるほど十分な回数繰り返されていません。
  - 高いエントロピーが観測されます。
  - ファイルの読み取り、書き込み、名前変更、または削除アクティビティが、通常のレベルと比較して 2 倍になりました。

SAN 環境の場合、警告は高エントロピーのみに基づきます。

証拠は、 ONTAPの Autonomous Ransomware Protection の情報に基づいています。詳細については、 "自律型ランサムウェア対策 - 概要" 。

アラート状態

アラート インシデントには、次の状態があります。

都道府県	説明
新しい	すべてのインシデントは、最初に特定されたときに「新規」としてマークされます。
レビュー中	アラートインシデントを評価するときに、手動で「レビュー中」としてマークすることができます。
却下	アクティビティがランサムウェア攻撃ではないと疑われる場合は、ステータスを「dismissed」に変更できます。+ 注意：攻撃を却下した後は、そのステータスを元に戻すことはできません。ワークロードを却下すると、潜在的なランサムウェア攻撃に応じて自動的に作成されたすべてのSnapshotコピーが完全に削除されます。
解決済み	インシデントは修正されました。
自動解決済み	優先度の低いアラートの場合、5日以内に何のアクションも取られなければ、インシデントは自動的に解決されます。

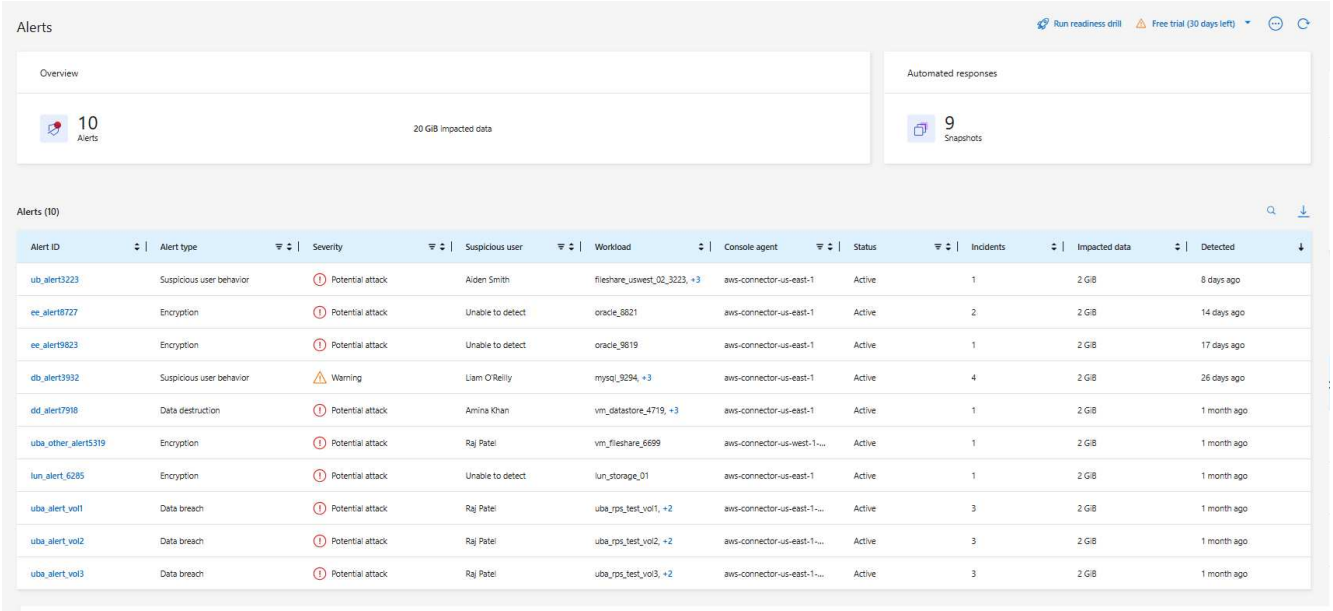
アラートを表示

アラートには、Ransomware Resilienceダッシュボードまたは*アラート*タブからアクセスできます。

必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアーのロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

1. NetApp Ransomware Resilienceダッシュボードで、[アラート]ペインを確認します。
2. いずれかのステータスの下にある*すべて表示*を選択します。
3. アラートを選択して、アラートごとに各ボリュームのすべてのインシデントを確認します。
4. 追加のアラートを確認するには、左上のパンくずリストで [アラート] を選択します。
5. 「アラート」ページでアラートを確認します。



6. 次のいずれかに進みます。
   - [悪意のあるアクティビティや異常なユーザー行動を検出する] 。
   - ランサムウェア インシデントを復旧準備完了としてマークする (インシデントが中和された後) 。
   - [潜在的な攻撃ではないインシデントを無視する] 。

アラートメールに返信する

Ransomware Resilienceは潜在的な攻撃を検出すると、NetApp Console設定で設定されたサブスクリプション通知設定に基づいて、登録ユーザーにメール通知を送信します。メールには、重大度や影響を受けるリソースなど、アラートに関する情報が記載されています。

コンソールで電子メール通知を設定するには、"メール通知設定を設定する"を参照してください。

必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、ランサムウェア レジリエンス管理者、またはランサムウェア レジリエンス ビューアーのロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

1. メールを表示します。
2. メールで*アラートを表示*を選択し、Ransomware Resilienceにログインします。

   アラート ページが表示されます。

3. 各アラートについて、各ボリュームのすべてのインシデントを確認します。
4. 追加のアラートを確認するには、左上のパンくずリストで [アラート] を選択します。
5. 次のいずれかに進みます。
    - [悪意のあるアクティビティや異常なユーザー行動を検出する] 。
    - ランサムウェア インシデントを復旧準備完了としてマークする (インシデントが中和された後) 。
    - [潜在的な攻撃ではないインシデントを無視する] 。

悪意のあるアクティビティや異常なユーザー行動を検出する

[アラート] タブを見ると、悪意のあるアクティビティや異常なユーザー動作があるかどうかを確認できます。

ユーザーレベルのアラートを表示するには、ユーザーアクティビティエージェントを設定し、ユーザー行動検出機能を備えた保護ポリシーを有効にする必要があります。アラートダッシュボードに「不審なユーザー」列が表示されるのは、ユーザー行動検出が有効になっている場合のみです。不審なユーザー検出を有効にするには、"不審なユーザーアクティビティ"をご覧ください。

悪意のあるアクティビティを表示する

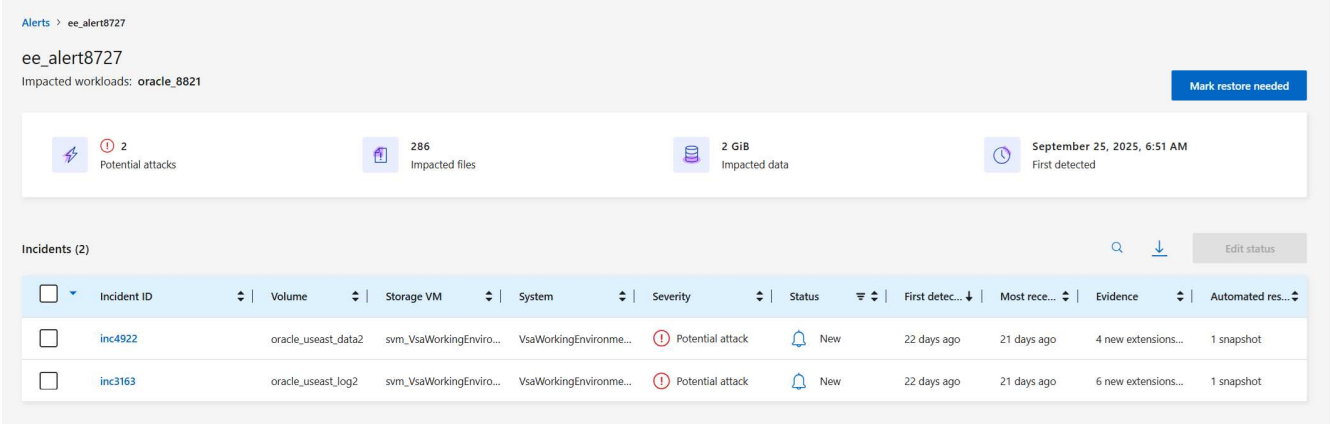
Autonomous Ransomware Protection が NetApp Ransomware Resilience でアラートをトリガーすると、次の詳細を表示できます：

- アラートがトリガーされたとき
- アクセスが変更または拒否された場合
- 受信データのエントロピー
- 新規ファイルの予想作成率と検出率の比較
- ファイルの予想削除率と検出率の比較
- 検出された率と比較したファイルの予想される名前変更率
- 影響を受けるワークロード、ボリューム、ファイル、ディレクトリ

> これらの詳細は、NAS ワークロードで表示できます。 SAN 環境では、エントロピー データのみが利用可能です。

手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。
2. アラートを選択します。
3. アラート内のインシデントを確認します。



4. インシデントの詳細を確認するには、インシデントを選択します。

異常なユーザー行動を表示する

異常なユーザー行動を表示するように疑わしいユーザー検出を設定している場合は、ユーザーレベルのデータを表示し、特定のユーザーをブロックできます。疑わしいユーザーの設定を有効にするには、"ユーザーアクティビティ検出用のエージェントとコレクターを設定する"を参照してください。

手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。
2. アラートを選択します。
3. アラート内のインシデントを確認します。
   a. 環境内の疑わしいユーザーをブロックするには、ユーザー名の横にある*ブロック*を選択します。
   b. 偽であるとわかっているアラートの対象となっている特定のユーザーに対するアラートを無効にするには、3つのドット(`…`を選択してから、このユーザーを監視から除外を選択します。ダイアログを確認し、除外を選択して確定します。

ユーザーのアラートを再度有効にするには、アラートを返します。3 つのドットを選択し、このユーザーを監視に含める を選択します。また、"ユーザーを除外する"監視から実行することもできます。

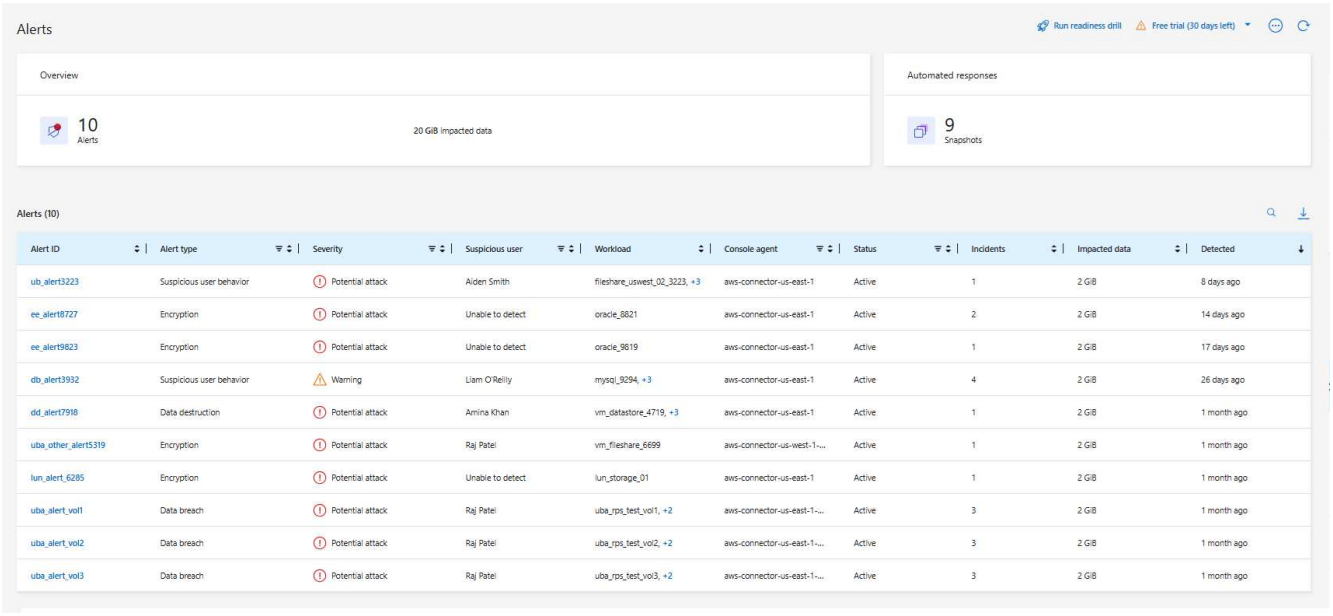
ランサムウェア インシデントを復旧準備完了としてマークする (インシデントが中和された後)

攻撃を停止した後、データの準備ができたことをストレージ管理者に通知し、リカバリプロセスを開始できるようにします。

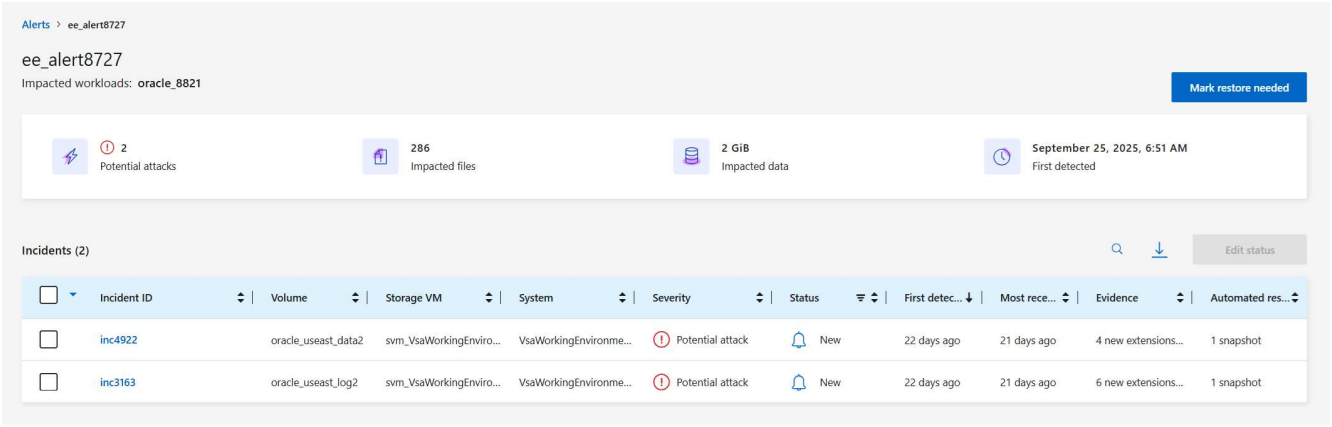
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。



2. 「アラート」ページで、アラートを選択します。
3. アラート内のインシデントを確認します。



4. インシデントの回復の準備ができていると判断した場合は、「復元が必要としてマーク」を選択します。
5. アクションを確認し、「復元が必要としてマーク」を選択します。
6. ワークロードの回復を開始するには、メッセージで「ワークロードの回復」を選択するか、「回復」タブを選択します。

結果

アラートが復元対象としてマークされると、アラートは [アラート] タブから [回復] タブに移動します。

潜在的な攻撃ではないインシデントを無視する

インシデントを確認した後、そのインシデントが潜在的な攻撃であるかどうかを判断する必要があります。実際の脅威ではない場合は、無視できます。

誤検知を無視するか、すぐにデータを回復することを決定できます。アラートを無視すると、Ransomware Resilience はこの動作を学習し、通常の操作と関連付けて、そのような動作に対して再度アラートを開始しなくなります。

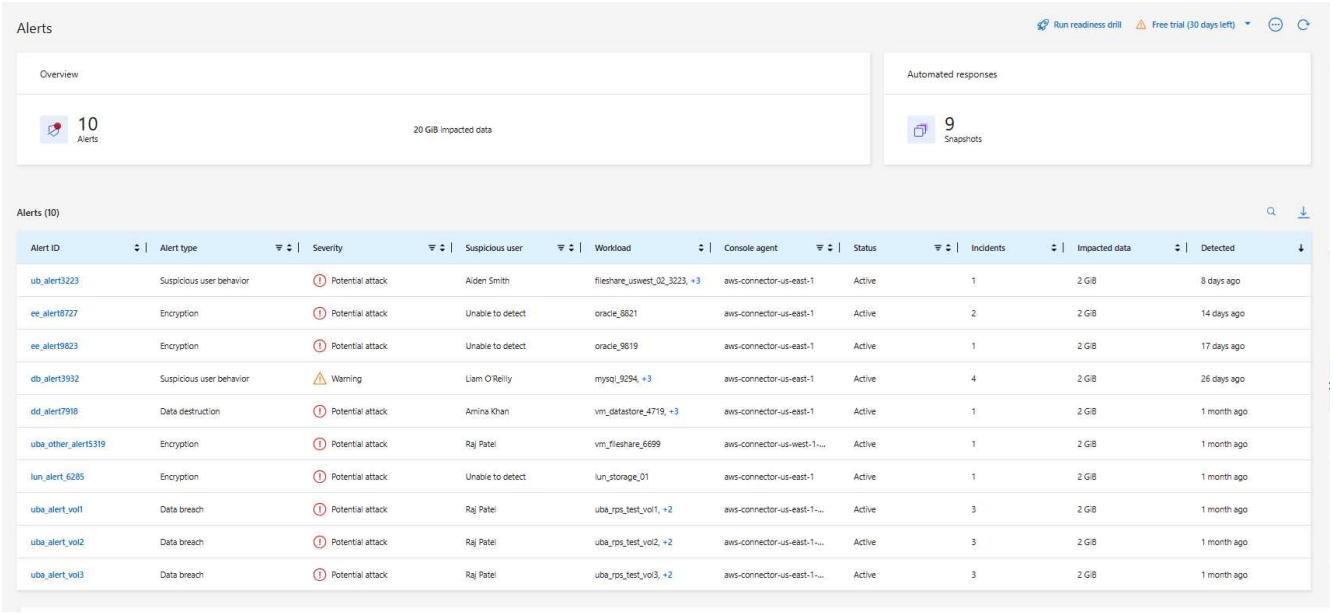
ワークロードを閉じると、潜在的なランサムウェア攻撃に応じて自動的に作成されたすべてのスナップショット コピーが完全に削除されます。

アラートを無視した場合、そのステータスを変更したり、この変更を元に戻したりすることはできません。

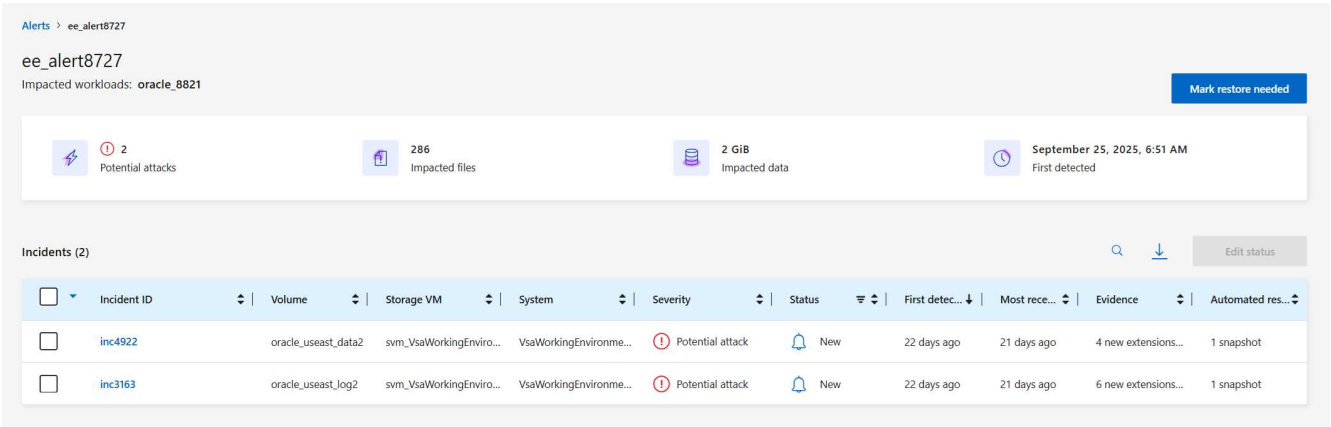
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

1. ランサムウェア耐性メニューから、「アラート」を選択します。

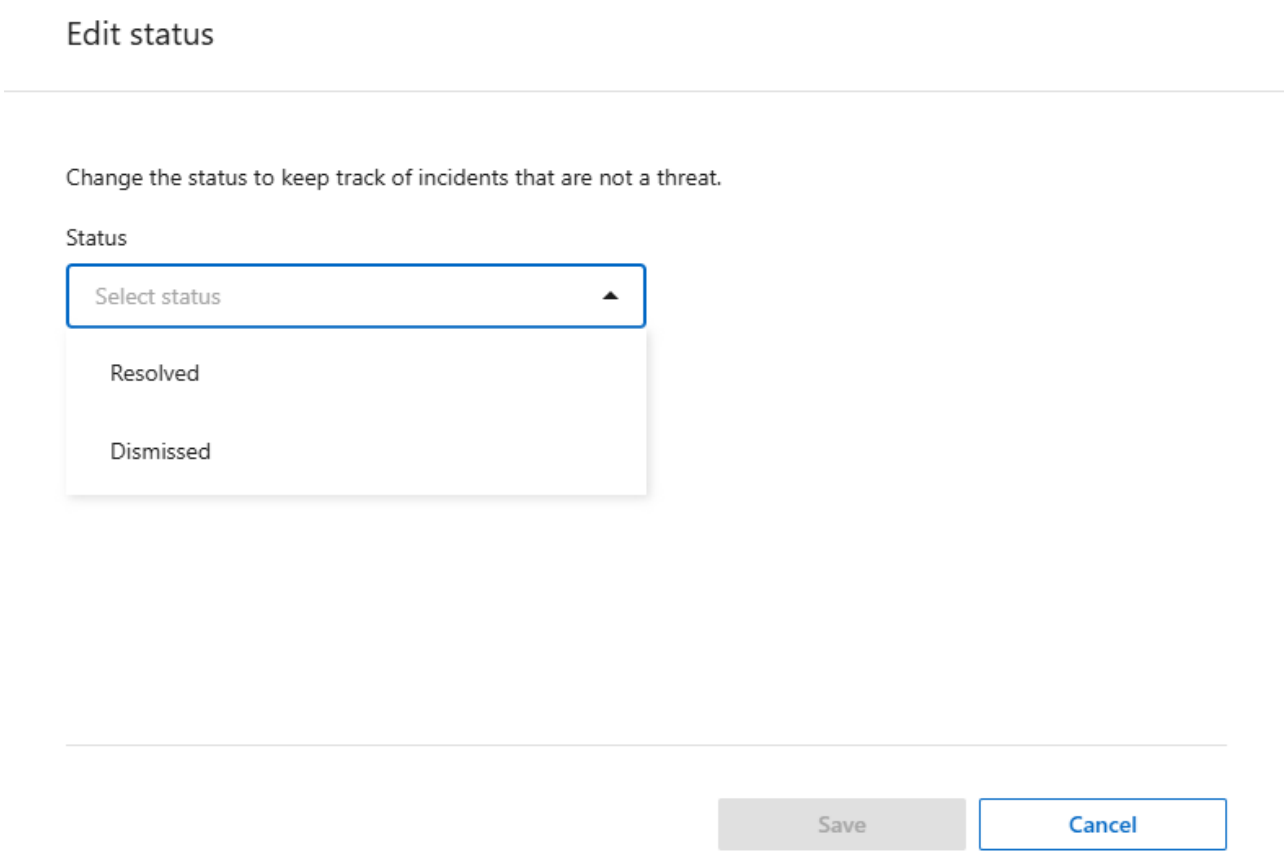


2. 「アラート」ページで、アラートを選択します。



3. 1 つ以上のインシデントを選択します。または、表の左上にあるインシデント ID ボックスを選択して、すべてのインシデントを選択します。
4. インシデントが脅威ではないと判断した場合は、誤検知として無視します。
   - インシデントを選択します。

◦ 表の上にある*ステータスの編集*ボタンを選択します。



5. [ステータスの編集] ボックスから、[却下] ステータスを選択します。

   ワークロードと削除されたスナップショット コピーに関する追加情報が表示されます。

6. *保存*を選択します。

   インシデントのステータスが「却下」に変わります。

影響を受けるファイルの一覧を表示する

アプリケーション ワークロードをファイル レベルで復元する前に、影響を受けるファイルの一覧を表示できます。影響を受けるファイルのリストをダウンロードするには、「アラート」ページにアクセスしてください。次に、「回復」ページを使用してリストをアップロードし、復元するファイルを選択します。

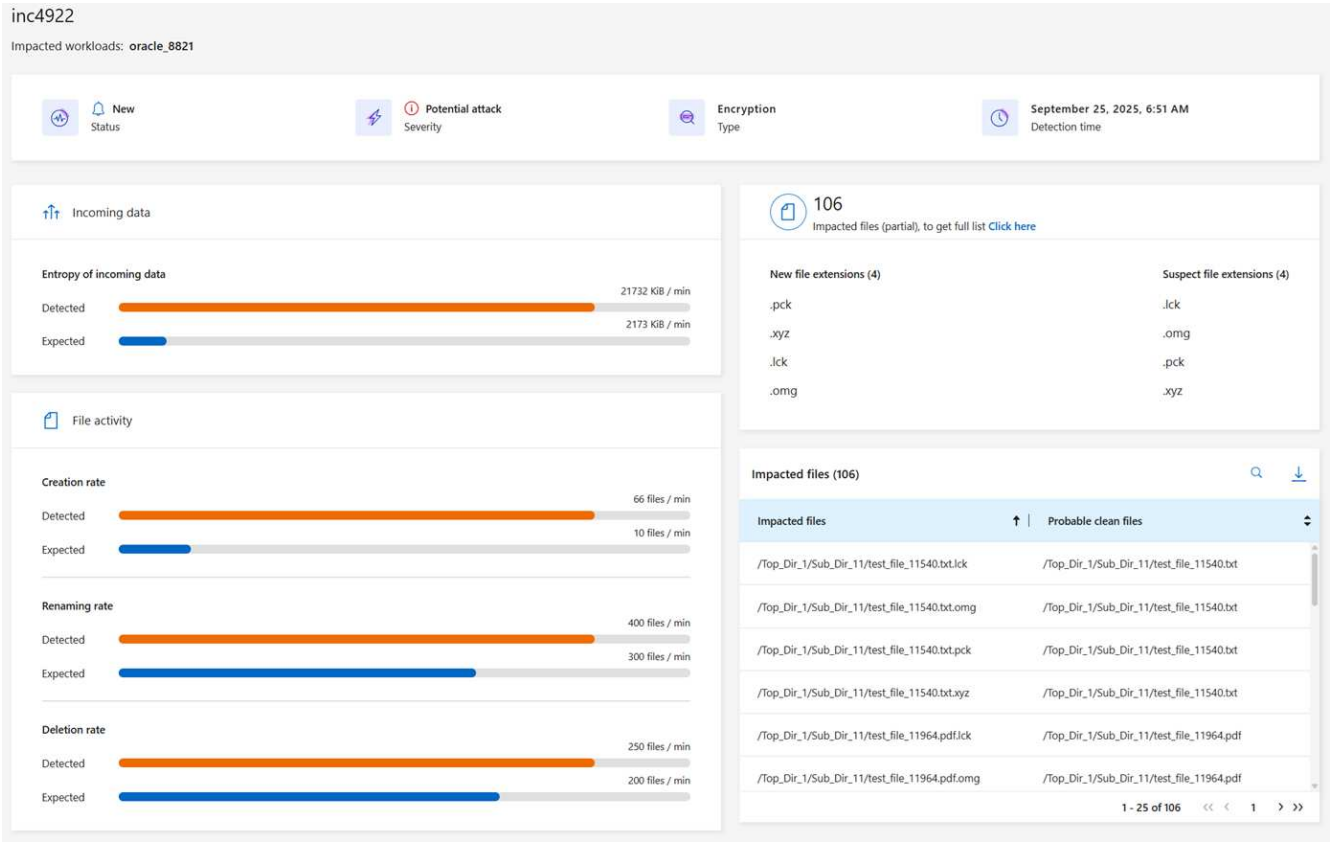
必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

手順

影響を受けるファイルのリストを取得するには、「アラート」ページを使用します。

ボリュームに複数のアラートがある場合は、アラートごとに影響を受けるファイルの CSV リストをダウンロードする必要がある場合があります。

1. ランサムウェア耐性メニューから、「アラート」を選択します。
2. [アラート] ページで、結果をワークロード別に並べ替えて、復元するアプリケーション ワークロードのアラートを表示します。
3. そのワークロードのアラートのリストから、アラートを選択します。
4. そのアラートに対して、単一のインシデントを選択します。



5. そのインシデントについては、ダウンロード アイコンを選択して、影響を受けるファイルのリストを CSV 形式でダウンロードします。

NetApp Ransomware Resilienceでリカバリステータスを確認

ワークロードが「復元が必要」とマークされた後、 NetApp Ransomware Resilience は実際のリカバリポイント (RPA) を推奨し、クラッシュ耐性のあるリカバリのワークフローを調整します。

- アプリケーションやVMがNetApp Backup and RecoveryまたはRansomware Resilienceによって管理されている場合、Ransomware Resilienceは「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態でリストアを実行します。これは、システムがクラッシュした場合など、同じ時点でボリューム内にあったすべてのデータがリストアされることを意味します。

  すべてのボリューム、特定のボリューム、または特定のファイルを選択してワークロードを復元できます。

ワークロードの回復は実行中のワークロードに影響を及ぼす可能性があります。適切な関係者と連携して回復プロセスを調整する必要があります。

ワークロードの復元ステータスは次のいずれかになります。

- 復元が必要です: ワークロードを復元する必要があります。
- 進行中: 復元操作が現在進行中です。
- 復元済み: ワークロードが復元されました。
- 失敗: ワークロードの復元プロセスを完了できませんでした。

復元準備が整ったワークロードを表示する

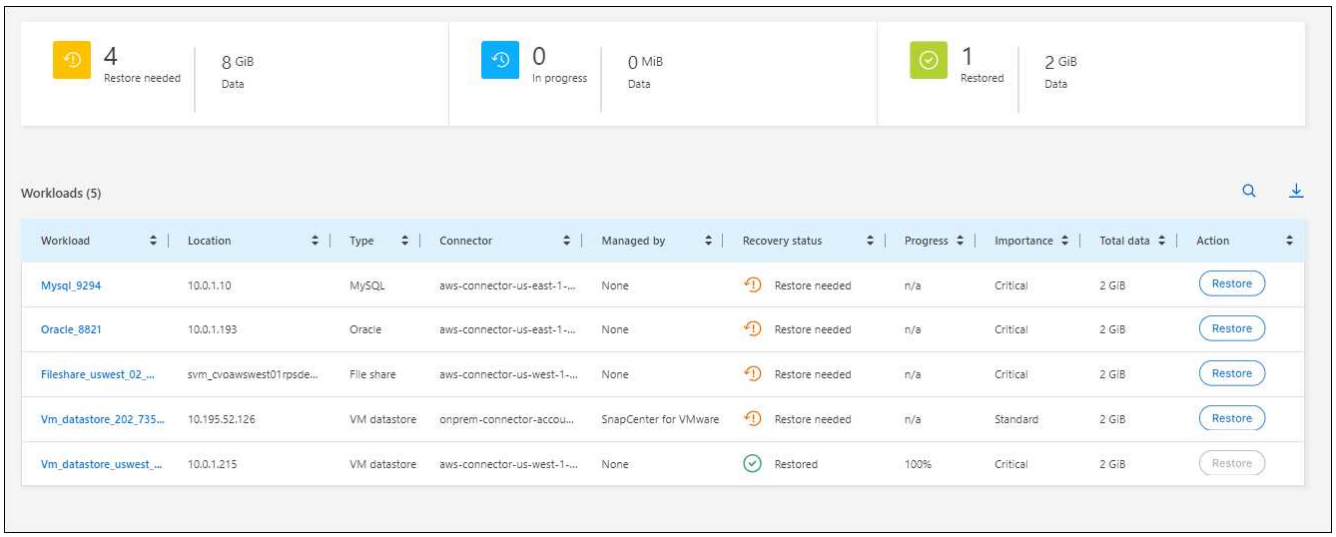
「復元が必要」の回復ステータスにあるワークロードを確認します。

手順

1. メインのRansomware Resilienceダッシュボードから、アラートペインの「復元が必要」の合計を確認し、*すべて表示*を選択します。

   または、サイドバーから * Recovery * を選択します。

2. *回復*ページでワークロード情報を確認します。



ワークロードをリカバリする

ワークロードを評価した後、ワークロードを復元するには次の2つの方法があります。

- カスタムリストアで復旧
- クリーンな復元で復旧

NetApp Ransomware Resilienceでリカバリステータスを確認

ワークロードが「復元が必要」とマークされた後、 NetApp Ransomware Resilience は実際のリカバリポイント (RPA) を推奨し、クラッシュ耐性のあるリカバリのワークフローを調整します。

- アプリケーションやVMがNetApp Backup and RecoveryまたはRansomware Resilienceによって管理されている場合、Ransomware Resilienceは「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態でリストアを実行します。これは、システムがクラッシュした場合など、同じ時点でボリューム内にあったすべてのデータがリストアされることを意味します。

  すべてのボリューム、特定のボリューム、または特定のファイルを選択してワークロードを復元できます。

ワークロードの回復は実行中のワークロードに影響を及ぼす可能性があります。適切な関係者と連携して回復プロセスを調整する必要があります。

ワークロードの復元ステータスは次のいずれかになります。

- 復元が必要です: ワークロードを復元する必要があります。
- 進行中: 復元操作が現在進行中です。
- 復元済み: ワークロードが復元されました。
- 失敗: ワークロードの復元プロセスを完了できませんでした。

復元準備が整ったワークロードを表示する

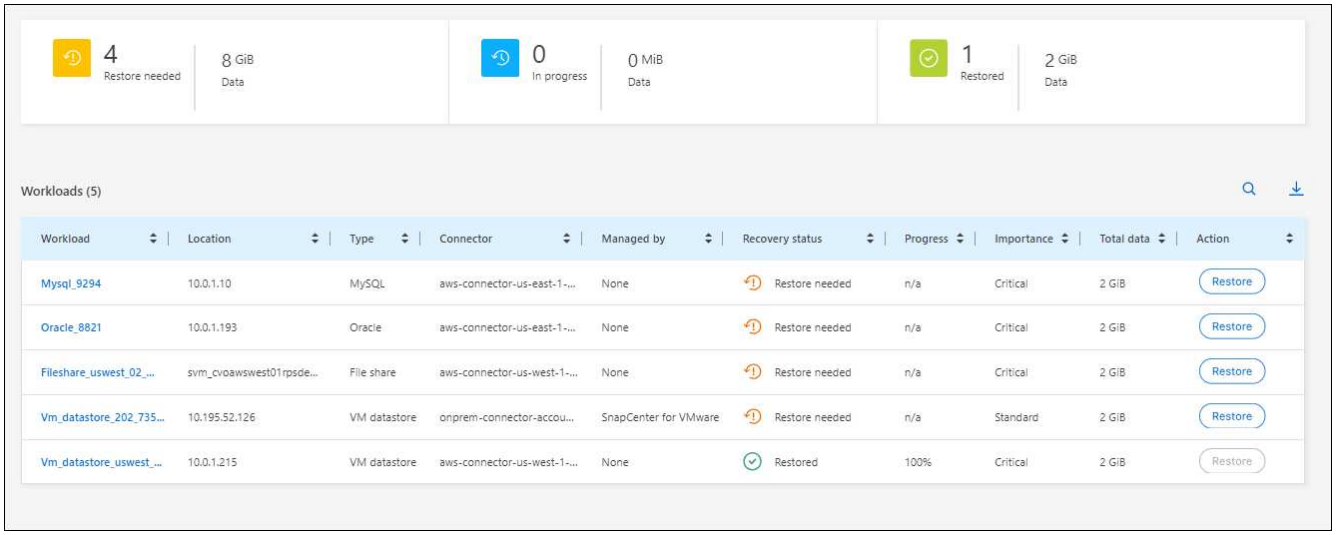
「復元が必要」の回復ステータスにあるワークロードを確認します。

手順

1. メインのRansomware Resilienceダッシュボードから、アラートペインの「復元が必要」の合計を確認し、*すべて表示*を選択します。

   または、サイドバーから * Recovery * を選択します。

2. *回復*ページでワークロード情報を確認します。



ワークロードをリカバリする

ワークロードを評価した後、ワークロードを復元するには次の2つの方法があります。

- カスタムリストアで復旧
- クリーンな復元で復旧

クリーンな復元を実行します

NetApp Ransomware Resilienceでクリーンリストアの環境を設定

NetApp Ransomware Resilienceはクリーンリストアを提供し、ランサムウェア攻撃後のガイド付きリカバリを実現します。クリーンリストアを実行するには、まずオンプレミスまたはサポートされているクラウド環境に、隔離されたリカバリ環境（IRE）を作成する必要があります。IRE内にクリーンルームを作成します。そこでRansomware Resilienceはワークロードを隔離し、どのファイルがクリーンで、どのファイルがランサムウェアの影響を受けているかを特定します。

必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

クリーンリストアについて

クリーンリストアを実行すると、NetApp Ransomware Resilienceがリカバリを最適化する複数ステップのプロセスをガイドします。

- セットアップ：クリーンなリストアを実行するには、まず IRE を作成し、次にリストアするワークロードを選択する必要があります。Ransomware Resilience は、ワークロードに関するすべてのアクションが実行されるクリーンルームを作成します。
- 分析：クリーンルームでは、NetApp Ransomware Resilienceがすべてのスナップショットを分析し、暗号化が存在するかどうかを確認します。クリーンな復元は、最適な復旧計画を決定するための復旧マップを作成します。

影響を受けるファイルを含まない復元ポイントが検出されると、それ以前のすべての復元ポイントはスキップされます。例えば、ランサムウェア攻撃が10月10日に発生し、10月7日午前10：21に影響を受けていない復元ポイントが見つかった場合、10月7日午前10：21より前のすべての復元ポイントはスキップされます。

分析ステップでは、レビューされたファイルの数も表示され、影響を受けるファイルと影響を受けないファイルが示されます。

- プラン：提供されている復旧オプションから選択してください。
  - 最新の影響を受けていない復元ポイント：攻撃前の最新の暗号化されていないスナップショットからの最も迅速な復元ポイント
  - データ損失最小：異なるスナップショットから得られた、暗号化されていないすべてのファイルの最新バージョン

    計画段階でファイル履歴を表示することで、ランサムウェア攻撃がファイルに影響を与えた時期や、復旧ポイントがその攻撃と時間的にどのように関連しているかを確認することもできます。
- クリーンアップ：NetApp Ransomware Resilience は、リカバリポイントからマルウェアを削除します。クリーンアップできないファイルがある場合は、復元対象から除外され、別の場所に隔離されます。
- 復元：NetApp Ransomware Resilienceは、クリーンなデータをソース環境に復元します。
- 終了：NetApp Ransomware Resilience はプロセスの詳細な概要を提供し、クリーンルームを閉じ、セットアップ中にプロビジョニングされたリソースを解放して、将来の従量課金コストを排除します。

サポートされている構成

- ランサムウェア対策アカウントごとに作成できるIREは1つだけです。各IREには3つのクリーンルームを設置できます。
- クリーン リストアは現在、 NAS ファイル共有（ NFS / CIFS ）でのみサポートされています。
- ソース環境にクリーン リストアを実行する必要があります。
- クラウドまたはオンプレミスでIREを作成できます。現在、以下の構成がサポートされています：

ソース	**Destination**（**IRE**）	サポートされている宛先リージョン
オンプレミス（AFF または FAS システムのみ）*	オンプレミス（VMware vCenter ）	該当なし
オンプレミス（AFF または FAS システムのみ）*	クラウド：AWS	• US East 1 • EU Central 1
クラウド：Cloud Volumes ONTAP と AWS*	クラウド：AWS	• US East 1 • EU Central 1
クラウド：Amazon FSxN for ONTAP	クラウド：AWS	• US East 1 • EU Central 1

* ONTAP 9.11.1以降を実行している必要があります。

クラウドベース環境でクリーンな復元を実行すると、クラウド プロバイダから追加のコンピューティング料金が発生する場合があります。詳細については、"コストとライセンス"を参照してください。

考慮事項

- 暗号化型ランサムウェア攻撃の場合、クリーンな復元のみを実行できます。
- 隔離された復旧環境に新しい操作を実行するための容量がない場合、空きができるまでキューに格納されます。
  - NetApp Ransomware Resilienceリカバリダッシュボードでは、アクティブなクリーン復元操作とキューに登録されているクリーン復元操作のステータスをいつでも監視できます。
- クリーンな復元を開始すると、元のボリュームがアンマウントされるため、IOアクセスが中断される可能性があります。

オンプレミス環境に関する追加の考慮事項

オンプレミスのIREを展開する場合、クリーンリストアでリカバリ分析のためにWindows VMをクローンすると、クローンされたVMはソースと同じ構成を保持します。これにより競合が発生する可能性があります：

- 同じセキュリティ識別子（SID）を使用すると、認証およびセキュリティ上の競合が発生します。
- 同じコンピュータ名（CN）を使用すると、ネットワークの競合が発生します。
- 同じマシン ID を使用すると、ライセンスとアクティベーションに関する問題が発生します。

これらの競合を回避するため、Ransomware ResilienceはクローンVMに対してsysprepを実行し、SID、CN、およびマシンIDをリセットします。これらの値をリセットすることで、クローンVMがソースVMに干渉することなく、独自の独立したインスタンスとして動作することが保証されます。

セカンダリ ソース

オンプレミスのソースに対してIREを作成する場合、セカンダリ ソースを追加するオプションがあります。

プライマリ ソースが利用可能な場合は、クリーン リストアをプライマリ ソースにリストアする必要があります。プライマリ ソースが利用できず、セカンダリ ソースを設定している場合は、クリーン リストアはセカンダリ ソースにリストアされます。

クリーンリストアプロセスは、デフォルトではソース環境のスナップショットを分析します。ソース環境が利用できない場合、またはソース上の暗号化されていないスナップショットが利用できない場合、クリーンリストアは、セカンダリ システムを設定済みの場合はそのスナップショットを分析します。

コストとライセンス

クリーン リストアは Ransomware Resilience の一部として提供されます。クリーン リストアの実行や IRE の作成に追加ライセンスは必要ありません。

クリーンリストアを有効にすると、サードパーティのクラウド プロバイダ料金が発生する可能性があります。サービスの利用方法によっては、クリーンリストア環境が存在する間、これらの料金が繰り返し発生する場合があります。

サードパーティの料金には、コンピューティング インスタンスの作成と導入、およびクリーニングとリカバリのための追加の本番ストレージ容量が含まれる場合があります。次の例を考えてみましょう：

- AWSにIREがデプロイされ、クリーンリストアを開始すると、暗号化とマルウェアをクリーンアップするために、IRE内のクリーンルームに2つのt3.medium AWS EC2インスタンスがデプロイされます。
- Cloud Volumes ONTAPでは、クリーン リストアによって、メタデータ ボリュームと分析用のSnapshotクローン用のクリーン ルーム ストレージVMが作成されます。

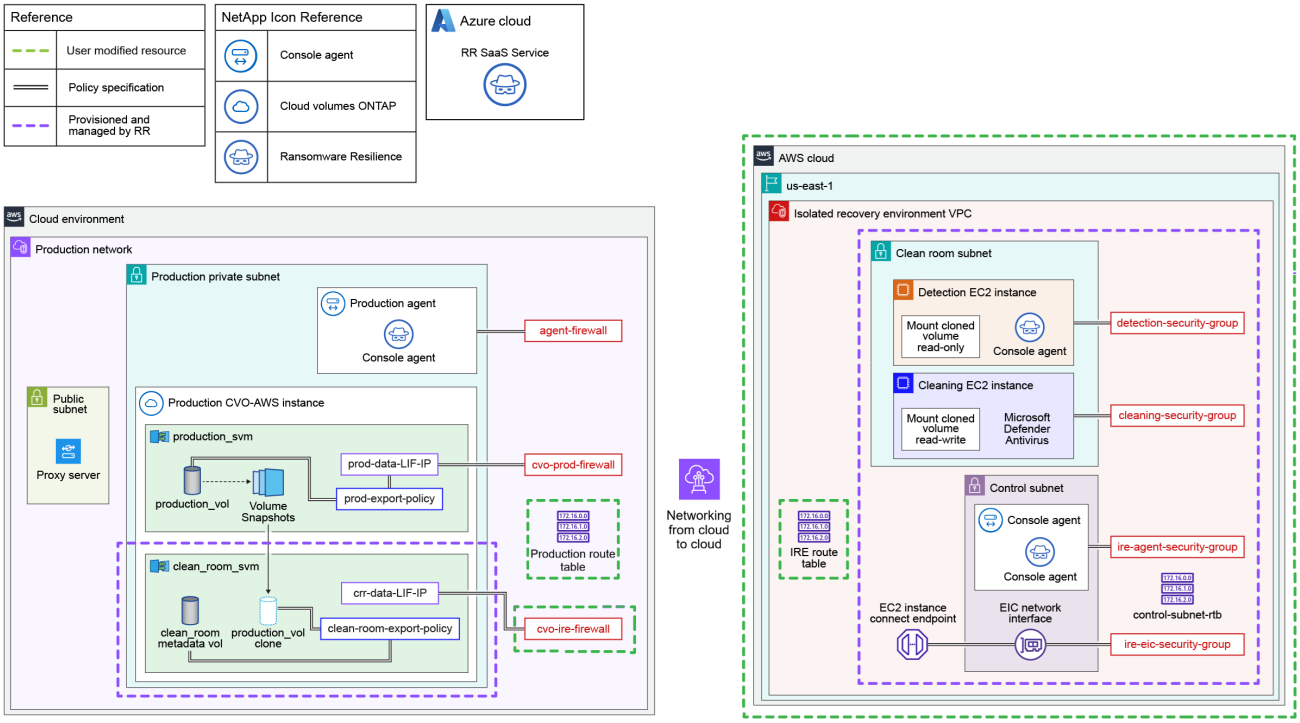
前提条件

選択したクリーン リストア導入タイプの前提条件が完了していることを確認してください。選択したIRE構成のタブを選択します。

IREを作成する際には、IRE作成時のシステム選択ステップで、分析に使用するすべてのシステム（プライマリまたはセカンダリ）を追加する必要があります。

クラウド間

この図は、クラウド間クリーンリストア構成の例を示しています。IREを作成する前に、図と構成する必要のあるリソースを確認してください。



クリーンルーム**SVM**データ**LIF IP**（**crr-data-LIF-IP**）

- クリーンルームSVMデータLIF用のIPアドレスを設定します。IPアドレスをメモしておいてください：このIPアドレスはIREの設定プロセス中に必要になります。
  - Cloud Volumes ONTAP with AWSでクラウド間クリーンリストアを使用する場合は、IPアドレスがElastic Network Interfaceに割り当てられていることを確認してください。
- SVMデータLIF IPからIREへのルーティングを許可します。

Amazon FSxN for ONTAP のソースで IRE を構成している場合は、このクリーンルーム SVM データ LIF IP 要件をスキップしてください。

本番環境ルートテーブル

- 本番環境のルーティングテーブルでは、IREサブネットからクリーンな復元データLIF IPへのトラフィックを許可する必要があります。このルートを本番環境のルーティングテーブルに追加する必要があります。
- 本番環境のONTAPクラスタのセキュリティグループとファイアウォールは、クリーンリストアデータLIF IPへのNFSv4およびNFSv3インバウンドトラフィックを許可する必要があります。ファイアウォールは、IRE CIDR範囲からのイングレスに対して開放されている必要があります（：）

プロトコル	宛先ポート	ソース	目的
TCP & UDP	2049	IRE VPC CIDR範囲	IREからのNFSv4アクセス

プロトコル	宛先ポート	ソース	目的
TCP & UDP	111	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	635	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	4045	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	4046	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	4049	IRE VPC CIDR範囲	IREからのNFSv3アクセス

IREルーティングテーブル

- IREルートテーブルは、IRE VPCのメインルートテーブルである必要があります。
- IREルーティングテーブルは、クリーンな復元データLIF IPアドレスへのルーティングを許可する必要があります。
- IREルーティングテーブルには、IREエージェントが動作するために、パブリックインターネットへのルートも含まれている必要があります。

仮想プライベートクラウド（**VPC**）

- IRE の場合は、本番環境の IP アドレス範囲内に VPC をプロビジョニングします。IP アドレスは、既存の IP アドレスと競合しないようにする必要があります。
  - VPCには最低64個のIPアドレス（/26ネットマスク）の容量が必要です。
  - VPCはパブリックインターネットアクセスを許可する必要があります。そうしないと、Consoleエージェントが動作しません。

クラウドの権限

- Ransomware Resilienceは、AWS環境でクリーンな復元を実行するために、適切なIAM権限を持つAWSアクセスキーとシークレットを必要とします。"AWSでIAMポリシーを作成する"以下の権限を付与した上で、ポリシーを新しく作成したユーザーに割り当ててください。ユーザーを作成したら、IAM認証情報を生成し、クリーン復元時にその情報を提供します。

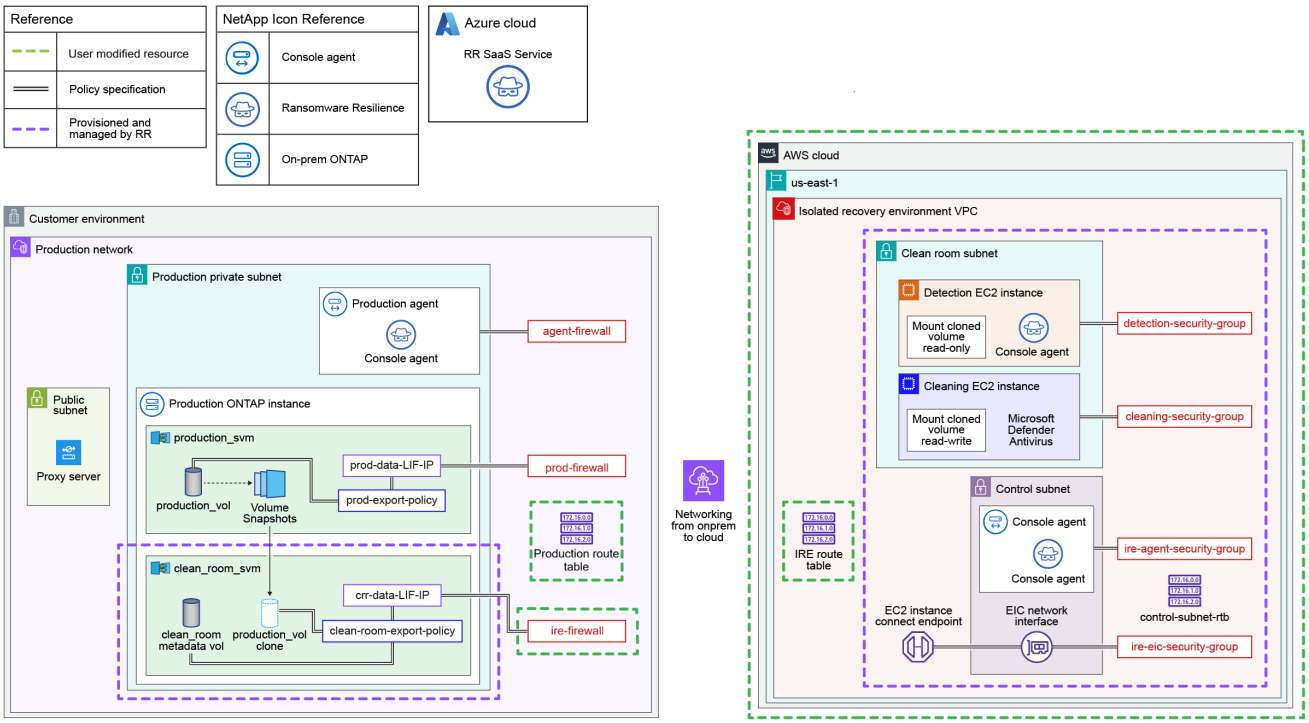
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Isolated recovery environmentFullAccess",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
```

```
                }
            }
        },
        {
            "Sid": "EC2CreateAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EC2ReadPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMFullAccess",
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
                }
            }
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketCreation",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketObjects",
            "Effect": "Allow",
            "Action": [
                "s3:*"
```

```
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket/*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucket",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket"
        }
    ]
}
```

オンプレミスからクラウドへ

この図は、オンプレミス環境からクラウド環境へのクリーンな復元構成の例を示しています。IREを作成する前に、図と構成する必要のあるリソースを確認してください。



クリーンルーム**SVM**データ**LIF IP**（**crr-data-LIF-IP**）

- クリーンルームSVMデータLIF用のIPアドレスを設定します。IPアドレスをメモしておいてください：このIPアドレスはIREの設定プロセス中に必要になります。
  - Cloud Volumes ONTAP with AWSでクラウド間クリーンリストアを使用する場合は、IPアドレスがElastic Network Interfaceに割り当てられていることを確認してください。

- SVMデータLIF IPからIREへのルーティングを許可します。

> Amazon FSxN for ONTAP のソースで IRE を構成している場合は、このクリーンルーム SVM データ LIF IP 要件をスキップしてください。

本番環境ルートテーブル

- 本番環境のルーティングテーブルでは、IREサブネットからクリーンな復元データLIF IPへのトラフィックを許可する必要があります。このルートを本番環境のルーティングテーブルに追加する必要があります。
- 本番環境のONTAPクラスタのセキュリティグループとファイアウォールは、クリーンリストアデータLIF IPへのNFSv4およびNFSv3インバウンドトラフィックを許可する必要があります。ファイアウォールは、IRE CIDR範囲からのイングレスに対して開放されている必要があります（：）

プロトコル	宛先ポート	ソース	目的
TCP & UDP	2049	IRE VPC CIDR範囲	IREからのNFSv4アクセス
TCP & UDP	111	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	635	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	4045	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	4046	IRE VPC CIDR範囲	IREからのNFSv3アクセス
TCP & UDP	4049	IRE VPC CIDR範囲	IREからのNFSv3アクセス

IREルーティングテーブル

- IREルートテーブルは、IRE VPCのメインルートテーブルである必要があります。
- IREルーティングテーブルは、クリーンな復元データLIF IPアドレスへのルーティングを許可する必要があります。
- IREルーティングテーブルには、IREエージェントが動作するために、パブリックインターネットへのルートも含まれている必要があります。

仮想プライベートクラウド（**VPC**）

- IRE の場合は、本番環境の IP アドレス範囲内に VPC をプロビジョニングします。IP アドレスは、既存の IP アドレスと競合しないようにする必要があります。
  - VPCには最低64個のIPアドレス（/26ネットマスク）の容量が必要です。
  - VPCはパブリックインターネットアクセスを許可する必要があります。そうしないと、Console エージェントが動作しません。

クラウドの権限

- Ransomware Resilienceは、AWS環境でクリーンな復元を実行するために、適切なIAM権限を持つAWSアクセスキーとシークレットを必要とします。"AWSでIAMポリシーを作成する"以下の権限を付与した上で、ポリシーを新しく作成したユーザーに割り当ててください。ユーザーを作成した

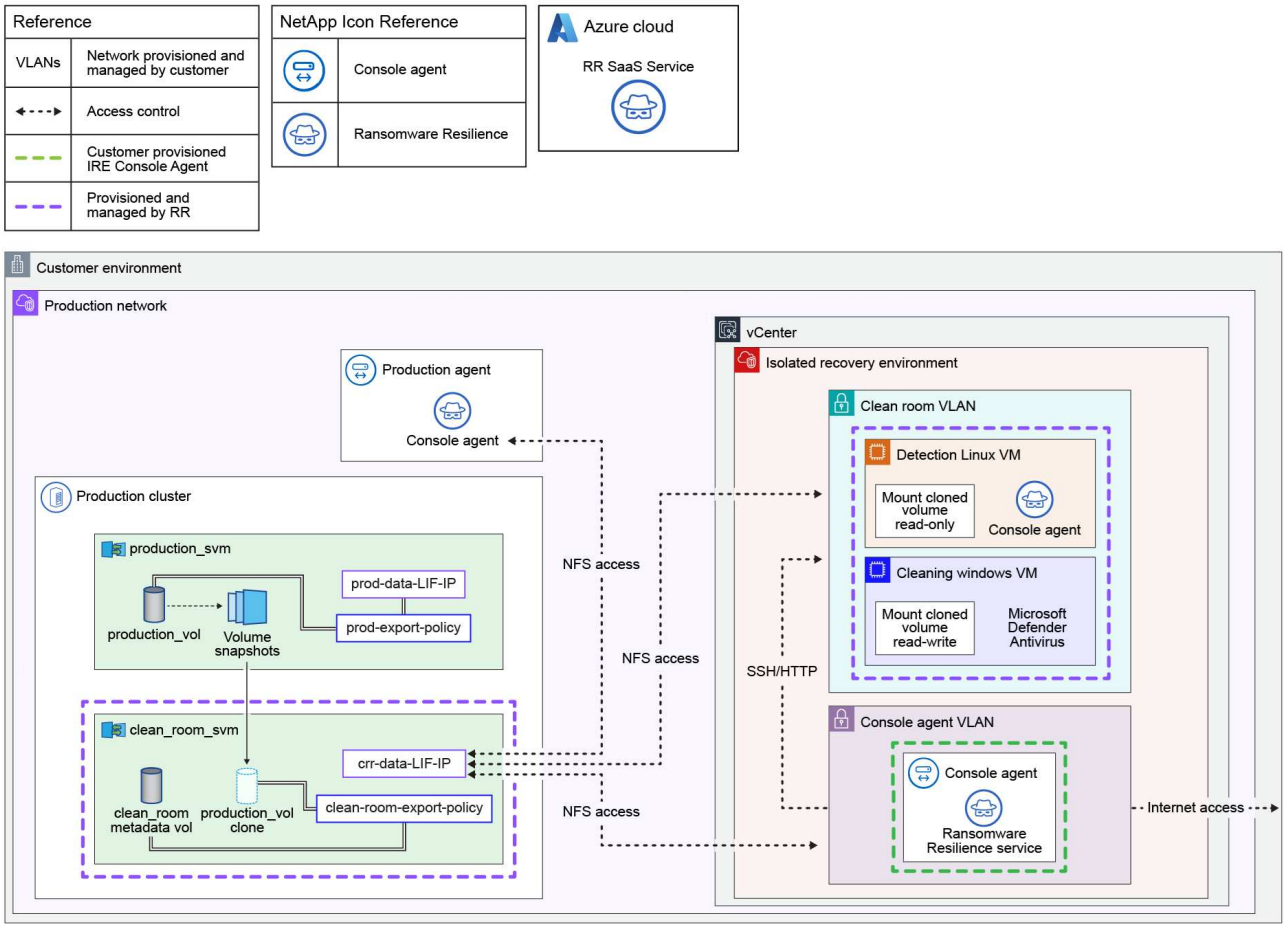
ら、IAM認証情報を生成し、クリーン復元時にその情報を提供します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Isolated recovery environmentFullAccess",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
                }
            }
        },
        {
            "Sid": "EC2CreateAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EC2ReadPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMFullAccess",
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
                }
            }
        },
        {
```

```
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketCreation",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketObjects",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket/*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucket",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket"
        }
    ]
}
```

オンプレミスからオンプレミス

この図は、オンプレミスからオンプレミスへのクリーン リストア構成の例を示しています。IREを作成する前に、図と構成する必要のあるリソースを確認してください。



クリーンルーム**SVM**データ**LIF IP**（**crr-data-LIF-IP**）

- ワークロードを復元するためにIREに接続するよう選択した各システムには、Storage Virtual Machine（SVM）が作成されます。クリーンルームSVMのデータLIFとして使用される各システムには、専用のIPアドレスを指定する必要があります。

ホストと**vCenter**

- vCenterのバージョンは7.0以降で、少なくとも1つのデータセンターが必要です。
- ESXi ホストは ESXi バージョン 7.0 以降である必要があり、少なくとも 1 台のホストには VM をクローンするのに十分な CPU とメモリリソースが利用可能でなければなりません。
- 提供されたvCenter認証情報には、リソースを検出して VM をクローニングするための権限が必要です。

ベース **VM**（**Windows** または **Linux**）

- クリーンリストアによる復旧時には、ベースとなる仮想マシンが選択されたデータセンターにクローンされ、選択されたESXiコンピューティング上に配置され、指定されたデータストアにマッピングされ、指定されたネットワークに接続されます。VMがクローンされると、2つのvCPUと4GBのRAM（LinuxまたはWindows VMの場合）、およびベースVMと同じ量のディスク容量を持つように構成されます。各クリーンリストアセッションでは、指定されたCIDR範囲から2つのIPアドレスが使用されます。
- 複数のクリーンルームセッションを同時に処理できるよう、十分なIPアドレス範囲を指定する必要があります。IPアドレスは復旧完了後に解放されます。
- データストアには、仮想マシンのクローン作成に対応できる十分な空き容量が必要です。

- IP アドレス範囲は CIDR 形式で指定する必要があります（例：100.100.0.0/24）
- Linux VMの場合：
  - オペレーティング システムは Ubuntu Linux 20.04 以降である必要があります。
  - オンプレミス システムの電源を入れる必要があります。
  - VMware Toolsがインストールされ、実行されている必要があります。
  - SSHが有効になっている必要があります。
  - nfs-commonをインストールする必要があります。
  - Dockerがインストールされ、実行されている必要があります。
  - 最低40GBの空き容量が必要です。
- Windows VMの場合：
  - Windows 仮想マシンには 20 GB の空き容量が必要です。
  - OS は Windows Server 2022 または 2025 である必要があります。
  - VMware Tools がインストールされ、実行されている必要があります。
  - WinRMを有効にする必要があります。
  - IP を設定する必要があります。
  - ベースVMのクローニングを許可する適切なライセンスがあることを確認してください。
  - VM の電源をオンにする必要があります。

ネットワーク

- VLAN リソースを次のアクセス権限で設定します：

リソース	アクセス
クリーンルーム SVM VLAN	NFSアクセス先：* Production Consoleエージェント * Console エージェントVLAN * クリーンルームVLAN
コンソール エージェント VLAN	• クリーン ルーム SVM VLAN への NFS アクセス • クリーンルーム VLAN への HTTP/SSH アクセス
クリーン ルーム VLAN	クリーン ルーム SVM VLAN への NFS アクセス

専用**NetApp Console**エージェント

- IRE 用の専用NetApp Console エージェントを導入します。Console エージェントは、クリーン ルーム VLAN にアクセスできる宛先vCenterに導入する必要があります。導入プロセスの詳細については、"オンプレミスに Console エージェントを導入する"を参照してください。

隔離された復旧環境を作成する

クリーンな復元を実行する前に、隔離されたリカバリ ルームを作成する必要があります。

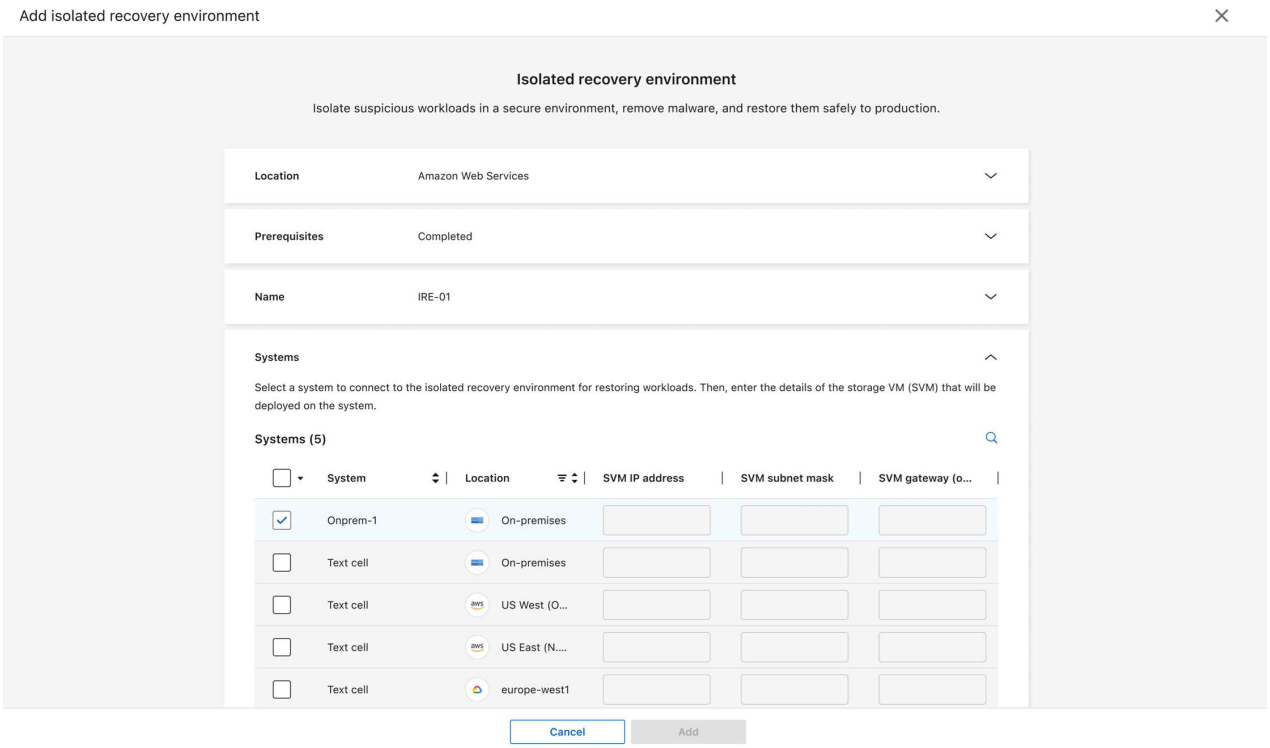
隔離されたリカバリ ルームを作成するプロセスは、環境がクラウドにあるかオンプレミスにあるかによって

異なります。正しい場所の手順に従ってください。

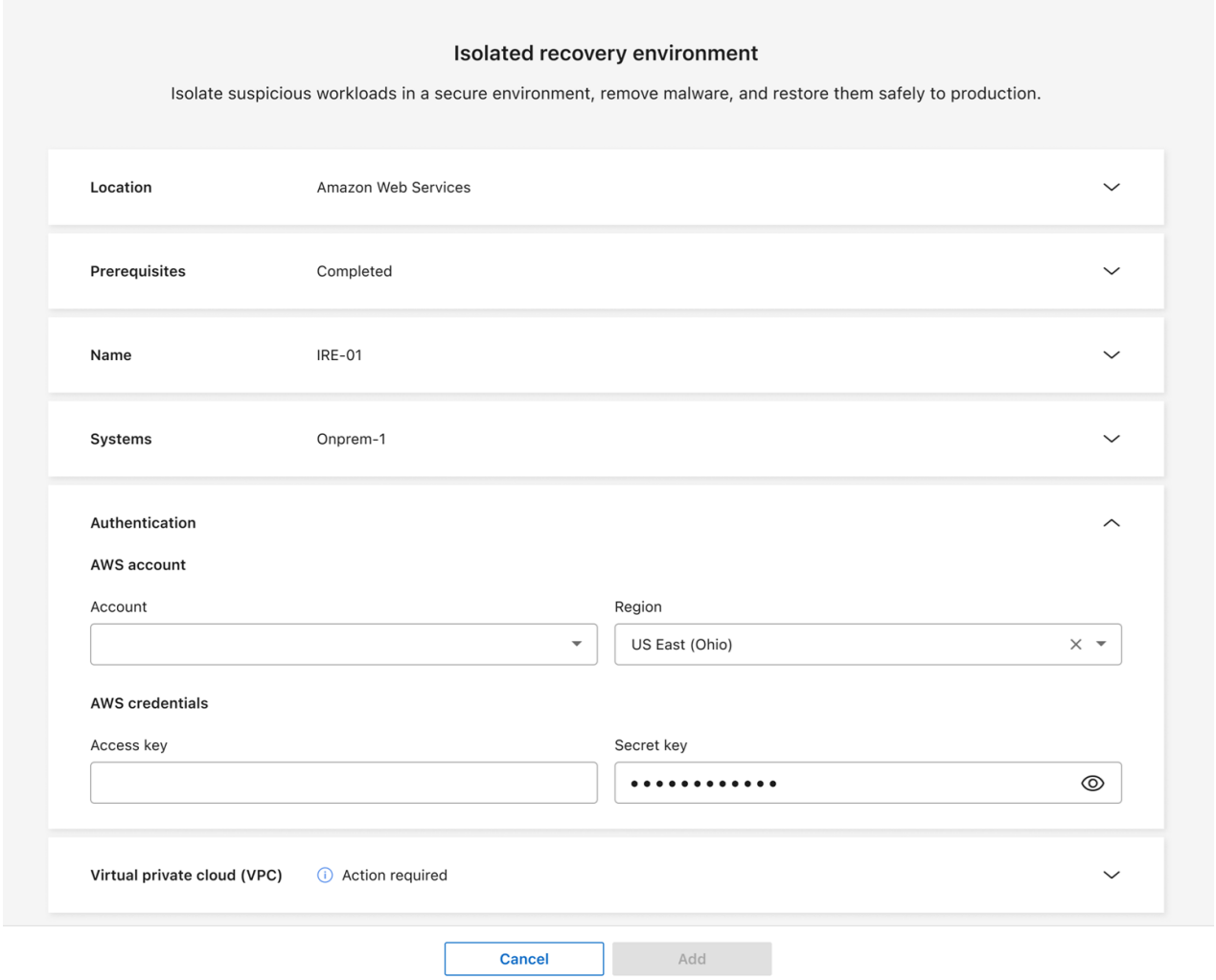
クラウド

1. ランサムウェア耐性で、[設定] を選択します。
2. クリーン復元カードで、追加を選択して、隔離された回復環境を作成します。
3. クラウドベースの IRE の場合は、**Amazon Web Services** を選択してください。
4. **Name** セクションを展開します。環境の **Name** を入力します。
5. *Systems*セクションを展開します。IRE に接続するシステムを選択します。選択した各システムについて、ストレージ VM の IP アドレス、サブネット マスク、およびゲートウェイを指定する必要があります。

> Amazon FSxN for ONTAPに導入されたIREの場合、この情報を提供する必要はありません。



6. * 認証 * セクションを展開します。
   - クラウドアカウントIDを入力し、ドロップダウンメニューからアカウントのリージョンを選択してください。IREはサポートされているリージョンにのみデプロイできます。
   - アカウントの**Access key**と**Secret key**を入力してください。
7. * Virtual private cloud （ VPC ）* セクションを展開します。IRE を導入する VPC ID を入力します。



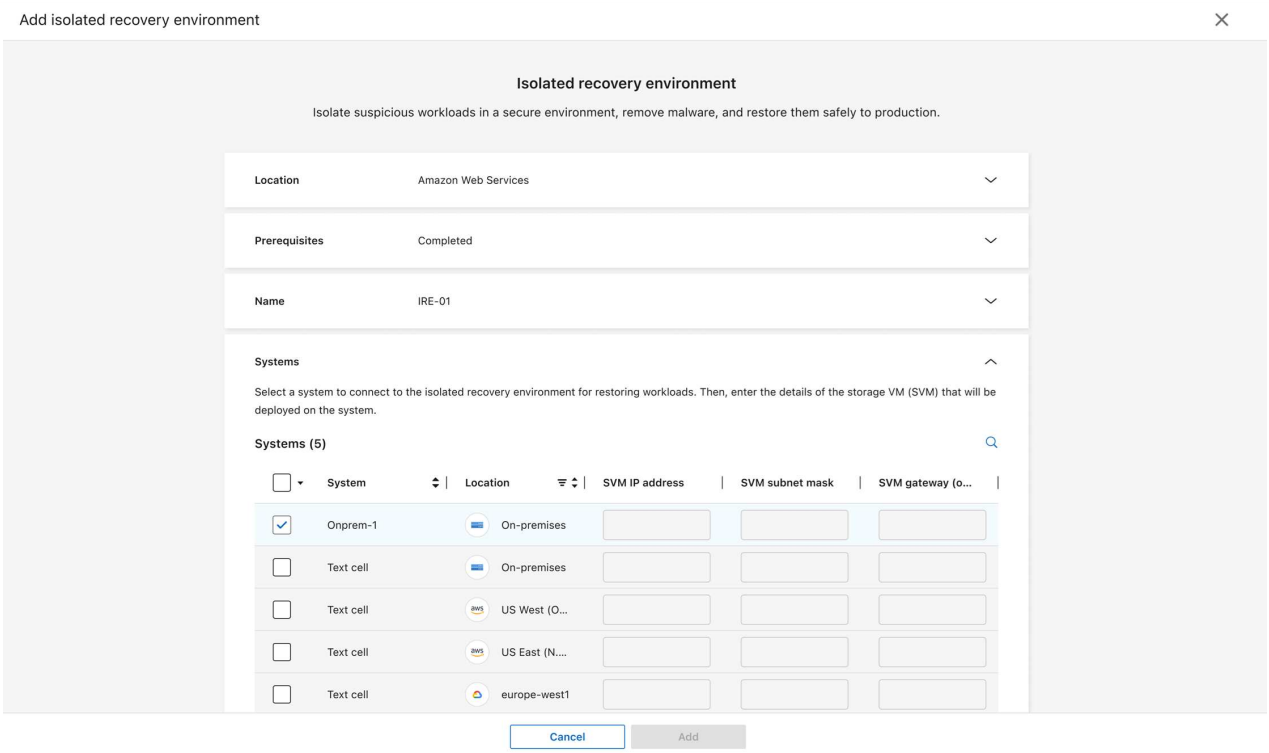
8. 追加を選択してIREを作成します。

   Ransomware Resilienceは、追加を選択した後に接続テストを実行します。これには数分かかる場合があります。IREのステータスが「deployed」と表示されれば、IREの展開は成功です。

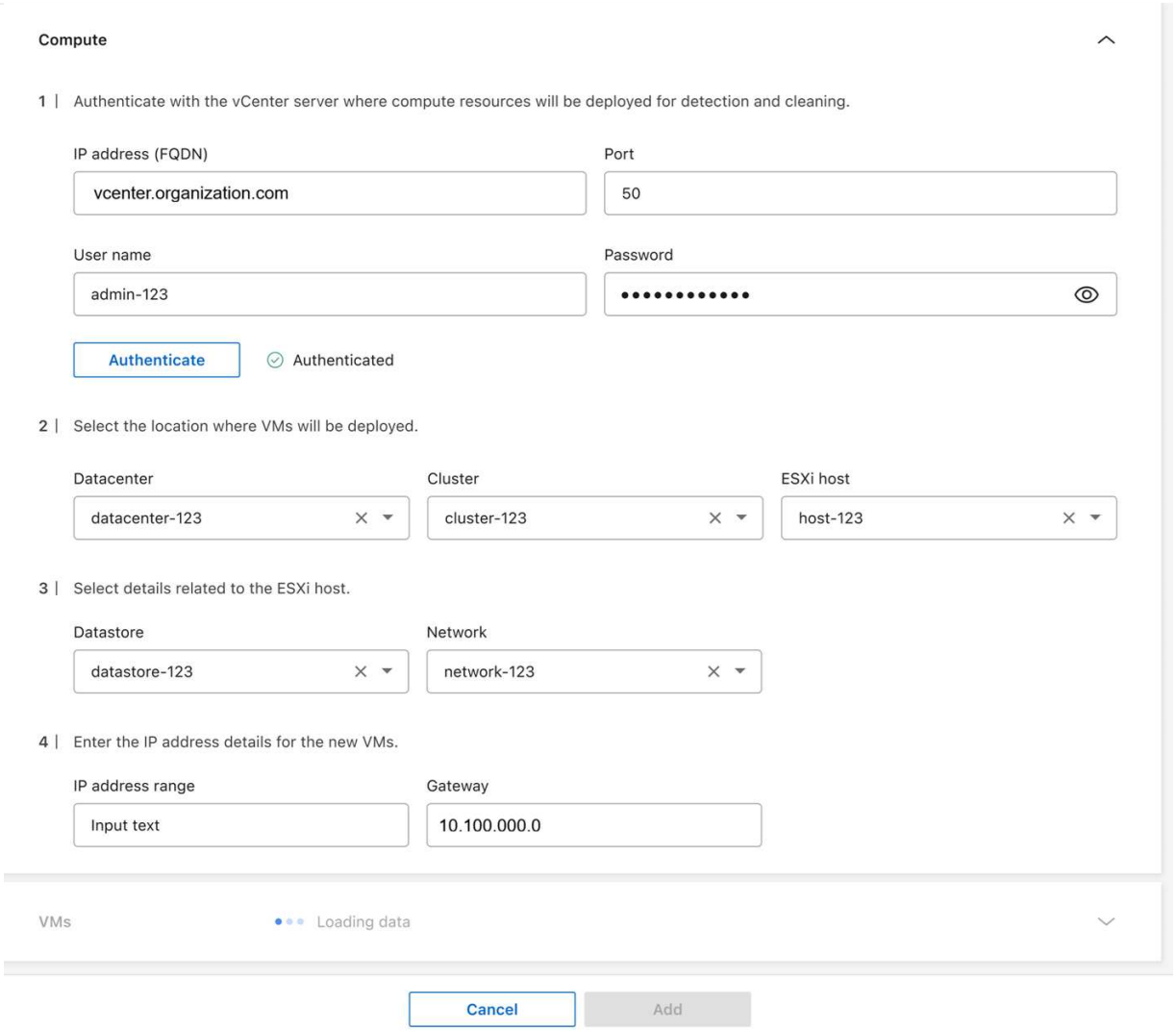
オンプレミス

1. ランサムウェア耐性で、[設定] を選択します。
2. 「クリーン復元」カードで、これが最初の環境の場合は 追加 を選択し、既に作成済みの場合は 管理 を選択します。
3. 場所については、オンプレミスを選択してください。
4. *Name*セクションを展開します。IREに**Name**を割り当てます。
5. *Systems*セクションを展開します。IREに接続するシステムを選択します。IREでリカバリするワークロードがある各システムに、ストレージVM IPアドレス、サブネットマスク、ゲートウェイを割り当てます。

   選択する各システムには、IPアドレスが割り当てられている必要があります。プライマリシステムまたはセカンダリシステムを選択できます。プライマリシステムに暗号化されていないスナップショットがない場合、またはプライマリシステムが利用できない場合は、セカンダリシステムを分析および復旧に使用できます。



6. **Console agent** セクションを展開します。IRE にデプロイされている Console agent をドロップダウンメニューから選択します。
7. **Compute** セクションを展開します。
   a. vCenter サーバーを認証するための認証情報を入力します：**IP** アドレス*または完全修飾ドメイン名（**FQDN**）、*ポート、ユーザー名、パスワード。
   b. 認証を選択してクレデンシャルを確認します。続行する前に、UIでクレデンシャルが確認されるまで待ちます。
   c. VM を導入する **Datacenter** と **Cluster** を選択します。
   d. ESXiホストの*データストア*と*ネットワーク*を選択します。
   e. VMの*IPアドレス範囲*をCIDR形式（例：10.0.0.1/24）、サブネットマスク、および*ゲートウェイ*を入力します。



8. *VMs*セクションを展開します。このセクションは、*Compute*セクションでの入力内容に基づいて入力されます。
   a. NetApp Ransomware Resilienceがランサムウェアのスキャンに使用するLinux VMについては、ドロップダウンメニューからVMを選択し、VMの*ユーザー名*と*パスワード*を入力してください。
   b. スキャンに使用するWindows VMについては、ドロップダウンメニューからVMを選択し、VMの*ユーザー名*と*パスワード*を入力します。
9. 追加を選択してIREを作成します。Ransomware Resilienceは、追加を選択した後に接続をテストします。この処理には数分かかることがあります。IREのステータスが「deployed」と表示されると、IREは正常に導入されています。

進捗状況を追跡できます。設定タブで、**Isolated recovery environments**を選択します。Isolated recovery environmentsページには、IREとそのステータスが表示されます。その環境に関連するすべてのジョブの詳細を確認するには、**View jobs**を選択してください。

IREは作成後でもシステムを変更できます。設定タブで、隔離されたリカバリ環境を選択します。編集したいIREを見つけて、アクションメニュー `...`を選択し、編集を選択します。システムの変更作業を進めてください。完了したら保存を選択してください。

IRE の詳細を変更する必要がある場合は、Ransomware Resilience サイドバーから **Settings** を選択し、Clean restore カードで **Manage** を選択します。IRE のアクションメニューを選択し、**Edit** を選択して設定を変更します。

隔離された回復環境を削除

復元操作がアクティブな状態では、IREを削除することはできません。復元操作をキャンセルするか、復元が完了するまで待ってからIREを削除してください。

IREを削除すると、クリーンルームSVMとメタデータボリュームも削除されます。これらのアセットが削除されると、クリーンリストアに関するレポートを生成することはできなくなります。

1. 設定に移動します。
2. 「クリーン復元」カードで、「管理」を選択します。
3. 削除するクリーンルームを特定します。IRE のアクションメニュー（(...）を選択し、削除 を選択します。
4. ダイアログで **Delete** を選択して操作を確定します。

NetApp Ransomware Resilienceでクリーンリストアを使用してワークロードをリカバリ

NetApp Ransomware Resilienceを使用すると、クリーンリストアを使用して、暗号化ベースのランサムウェア攻撃のあとにガイド付きリカバリを実行できます。クリーンリストアは、データ損失を最小限に抑え、ワークロードを可能な限り短時間でオンラインに戻すための最適化されたリカバリパスを特定します。

開始する前に

必要なコンソール ロール このタスクを実行するには、組織管理者、フォルダーまたはプロジェクト管理者、またはランサムウェア耐性管理者のロールが必要です。"NetApp Consoleのランサムウェア耐性ロールについて学ぶ" 。

クリーンな復元を実行する前に、"隔離された回復環境"を設定しておく必要があります。

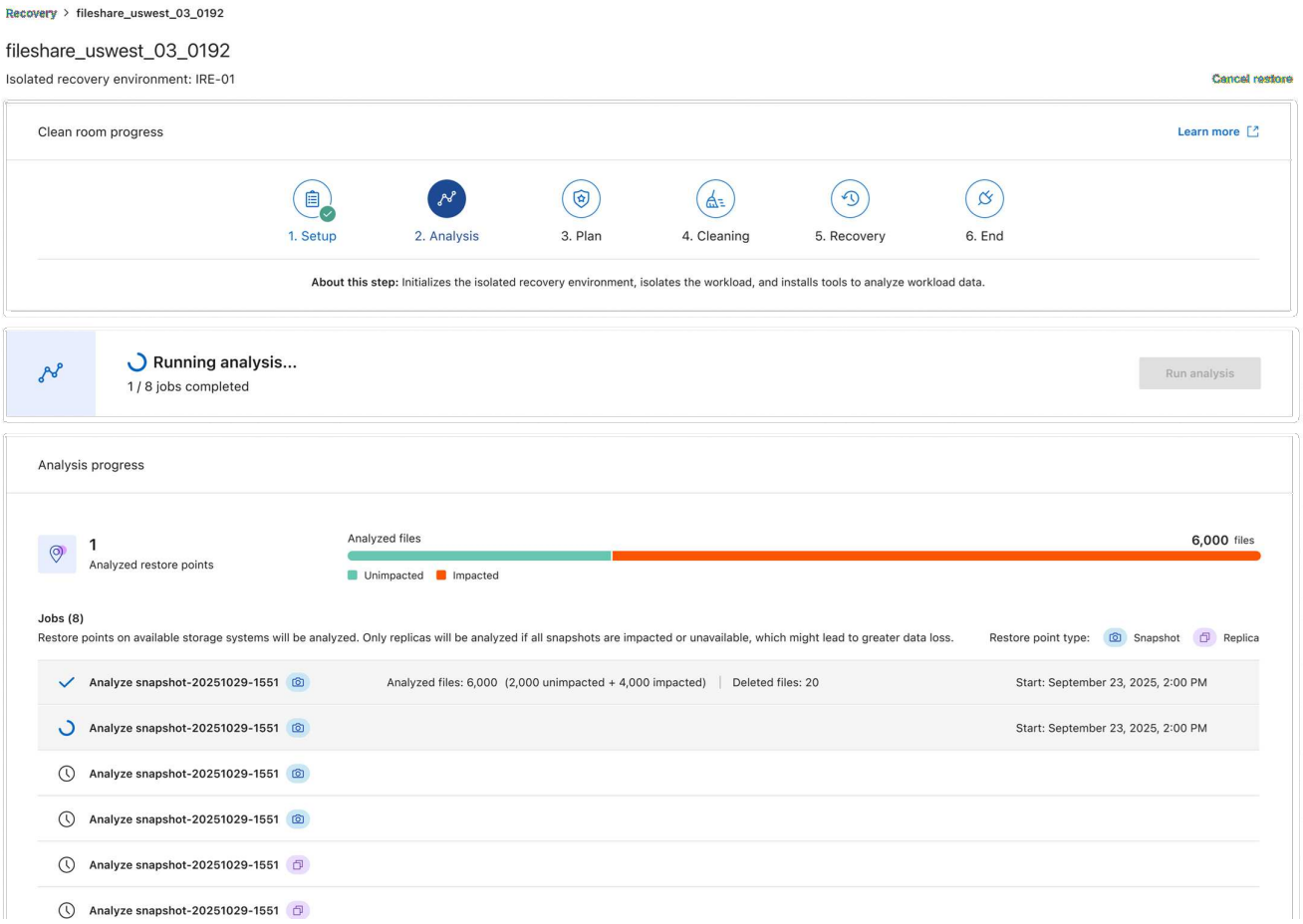
考慮事項

- 暗号化型ランサムウェア攻撃の場合、クリーンな復元のみを実行できます。
- 隔離された復旧環境に新しい操作を実行するための容量がない場合、空きができるまでキューに格納されます。
  - NetApp Ransomware Resilienceリカバリダッシュボードでは、アクティブなクリーン復元操作とキューに登録されているクリーン復元操作のステータスをいつでも監視できます。
- クリーンな復元を開始すると、元のボリュームがアンマウントされるため、IOアクセスが中断される可能性があります。

クリーンな復元を実行します

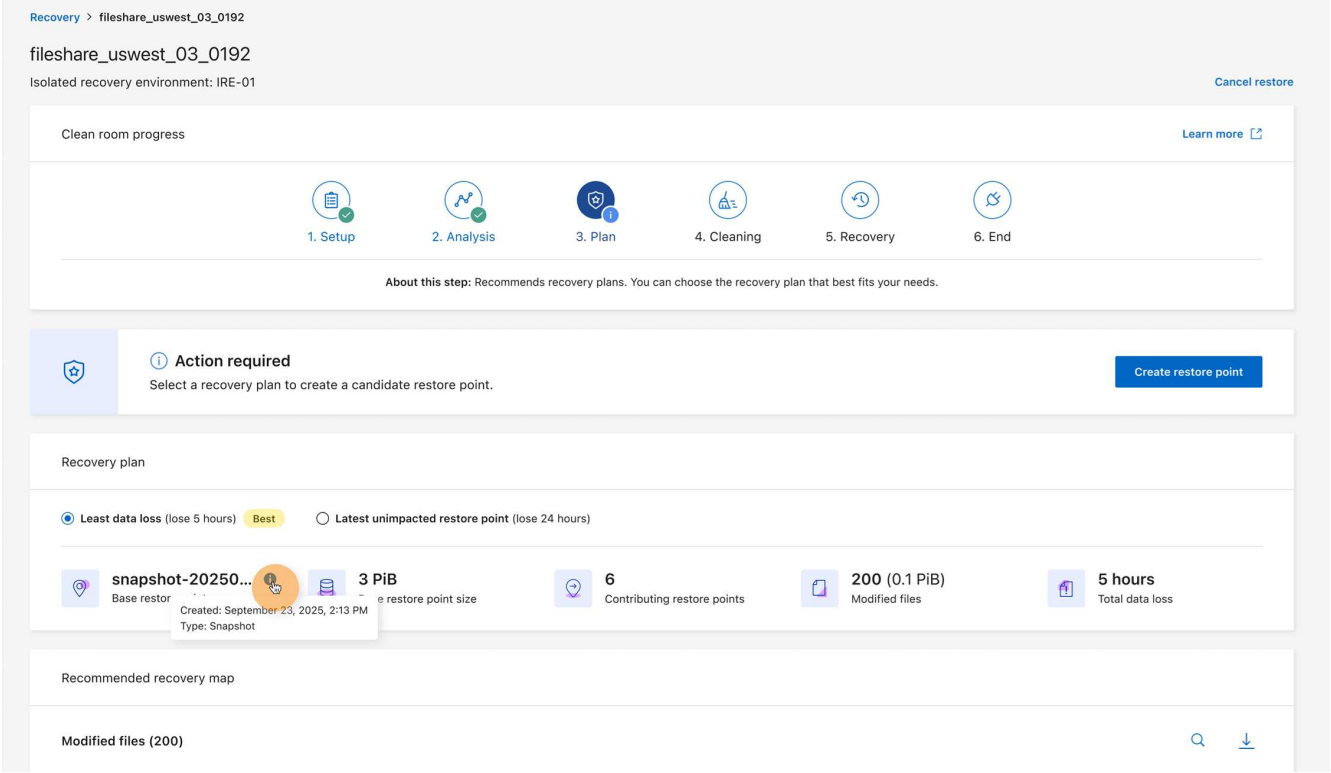
1. **Recovery**セクションで、復元するワークロードを選択します。**Restore**を選択します。

2. 復元タイプのオプションで、クリーン復元を選択し、次へをクリックします。
3. 使用する隔離されたリカバリ環境を選択し、*[次へ]*をクリックします。
4. 隔離された復旧環境を確認し、正しい場所であることを確認します。**Restore**を選択します。
5. Ransomware Resilienceは必要な設定を実行します。セットアップが正常に完了すると、Ransomware Resilience は**Setup complete**と表示します。分析に進むには、**Next**を選択してください。
6. セットアップが完了したら、分析を実行を選択してください。Ransomware Resilienceは、ランサムウェア攻撃発生前の7日間に利用可能なすべての復元ポイントを分析し、復元ポイントの日付と種類を表示します。



7. 分析が完了したら、**Next**を選択して回復計画を立ててください。Ransomware Resilienceには、**Least data loss**と**Latest unimpacted restore point**という2つのオプションがあります。いずれかのオプションを選択し、必要に応じて、それぞれの復元ポイントの個々のファイルデータを確認できます。

   詳細なファイルイベントデータを表示するには、分析対象のファイルを選択して暗号化ステータスを確認します。ファイルが作成、変更、または削除された日時、およびどの復元ポイントがどの操作に対応するかを確認できます。



8. 復元ポイントを選択したら、次へを選択してファイルのクリーンアップを開始してください。
9. Ransomware Resilienceがワークロードのクリーンアップを開始します。

   クリーニングが完了したら、**Start recovery**を選択してリカバリを開始します。

10. 元のワークロードを保存するかどうかを選択してください。元のワークロードを保存しない場合は、**No, replace the original workload**を選択してください。保存するには、**Yes, save the original workload**を選択し、ワークロードの新しい名前を入力します。
11. リカバリ開始を選択して、リカバリを開始します。
12. リカバリが完了したら、**Next**を選択して最終フェーズに進みます。
13. リソースを解放して終了を選択して、リソースを解放し、クリーンルームを閉じます。リソースを解放することを確認するには、終了を選択します。

著作権に関する情報

商標に関する情報